**UNITED STATES DISTRICT COURT**
**FOR THE NORTHERN DISTRICT OF OHIO**
**EASTERN DIVISION AT CLEVELAND**

**DANIEL BOZIN, as Executor of the Estate of AURORA MURGU, JAMES MCNICHOL, JESSICA MCNICHOL, KRISTI BURK, and PATRICIA BURK, individually and on behalf of all others similarly situated,**

Plaintiffs,

v.

**KEYBANK, N.A.**
% Christopher M. Gorman, C.E.O,
127 Public Square
Cleveland, OH 44107

AND

**OVERBY-SEAWELL CO.**
% Corporation Service Company,
Registered Agent
2 Sun Court, Suite 400
Peachtree Corners, GA 30144

Defendants.

Case No. 1:22-cv-1536-CEF

**FIRST AMENDED CLASS ACTION COMPLAINT**

**DEMAND FOR JURY TRIAL**

Plaintiffs DANIEL BOZIN, as Executor of the Estate of Aurora Murgu, and individually, JAMES MCNICHOL, JESSICA MCNICHOL, KRISTI BURK, and PATRICIA BURK, individually on behalf of all others similarly situated (collectively, "Plaintiffs"), through their attorneys, bring this action against Defendants KeyBank, N.A. ("KeyBank"), and Overby-Seawell Co. ("OSC") (collectively, "Defendants"), and allege upon personal knowledge as to their own actions and experiences, and upon information and belief as to all other matters, as follows:

## INTRODUCTION

1. This consumer data breach lawsuit arises out of Defendants' unreasonable, unlawful, and unfair practices with regard to their collection and maintenance of the highly sensitive and confidential mortgage information (the "PII"). Defendants' insufficient and unreasonable data security practices caused, facilitated, and exacerbated the data breach (the "Data Breach") and its impact on Plaintiffs and Class members. By Defendants' own admission, starting on July 5, 2022, unauthorized external parties gained remote access to OSC's network and acquired certain information from OSC's clients, including KeyBank.

2. The Data Breach exposed Plaintiffs' and Class members' highly personally identifiable information and financial information ("PII") to criminals, including their names, addresses, loan numbers, and Social Security numbers. For some unspecified Class members, additional loan information was also stolen by the criminals.

3. The PII that Defendants compromised, exposed, and criminals stole in the Data Breach consists of some of the most sensitive and damaging information when in the hands of criminals, including but not limited to: names, mortgage property address, mortgage account number(s) and mortgage account information, phone number, property information, 8-digits of Social Security numbers, and home insurance policy number and home insurance information. Moreover, the information relates to what is for many the single most important asset, both subjectively and objectively—their home.

4. The PII stolen in the Data Breach can be used by criminals alone, and in conjunction with other pieces of information, to perpetrate crimes against Plaintiffs and Class members that can result in significant liability and damage to their money, property, creditworthiness, reputation,

and their ability to pay current loans, improve their credit, and/or obtain loans on favorable terms in the future.

5. Plaintiffs and Class members entrusted Defendants with an extensive amount of their sensitive PII. Defendants understand the importance of protecting such information and tout their cybersecurity capabilities as a selling point. For example, in its website Privacy Policy[1], OSC states:

> The privacy of personal client information is important to Breckenridge IS, LLC, and its subsidiaries and affiliates (collectively "Breckenridge IS" including the Overby-Seawell Co. called "OSC"). Under Federal law, any financial institution, directly or through its affiliates, is generally prohibited from sharing nonpublic personal information about consumers or customers with a nonaffiliated third party unless the institution provides such consumer or customer with a notice of its privacy policies and practices, such as the type of information that it collects from consumers and customers and the categories of persons or entities to whom the information may be disclosed. In compliance with Federal law and the state laws relating to privacy in the insurance industry, and in order to notify our clients of our privacy policies and practices, we have established this Privacy Policy.
>
> * * *
>
> **Confidentiality and Security of Information**
>
> We restrict access to nonpublic personal information about Participants to those employees of Breckenridge IS and OSC who need to know that information in order to provide products or services to our Participants. We have in place physical, electronic, and procedural safeguards in order to protect any nonpublic personal information we maintain regarding our Participants.
>
> **Professional Standards**
>
> Whatever the legal environment, we have constantly held ourselves to the highest of professional standards. At Breckenridge IS and OSC, we strive always to maintain the highest level of confidentiality for our Participants.

[1] https://www.oscis.com/privacy/

6. Similarly, KeyBank represents that "we take the security of your data and information seriously. That's why we use sophisticated tools, technology and training to keep the information you entrust to us safe, protected and secure."[2] To safeguard your information, we also use:

- ✓ Industry-leading cybersecurity tools, practices and technology
- ✓ Multifactor identification practices that protect clients' identities
- ✓ Our Cyber Defense Center, which tracks the latest threats
- ✓ Our Fraud Prevention Services group, which monitors client accounts proactively for suspicious activity.[3]

7. These representations concerning data security were false. On July 5, 2022, criminals breached Defendants' systems, and accessed, and acquired electronic files containing the PII of Plaintiffs and Class members. The criminals gained unauthorized access by thwarting, circumventing, and defeating Defendants' unreasonably deficient data security measures and protocols.

8. Plaintiffs, individually, and on behalf of all persons similarly situated, seeks to be made whole for the losses incurred by the victims of the Data Breach, and the losses that will be incurred in the future. Plaintiffs also seek injunctive relief in the form of compliant data security practices, full disclosure regarding the disposition of the information in Defendants' systems, and monitoring and audits of Defendants' security practices going forward because Defendants continue to collect, maintain, and store Class members' PII and home loan data.

[2] https://www.key.com/about/security/privacy-security.html
[3] *Id*.

## PARTIES, JURISDICTION, AND VENUE

9. Plaintiff Daniel Bozin is a citizen of Ohio, and the executor of the estate of Aurora Murgu. Ms. Murgu's residential home loan was secured by a mortgage originated and/or serviced by Defendants.

10. Plaintiff James McNichol is a citizen of New York, and his residential home loan is secured by a mortgage originated and/or serviced by Defendants.

11. Plaintiff Jessica McNichol is a citizen of New York, and is the spouse of Plaintiff James McNichol. Her PII was in Defendants' possession at the time of the Data Breach, as Defendants had previously requested her PII in connection with Mr. McNichol's residential mortgage loan.

12. Plaintiff Kristi Burk is a citizen of Georgia and she, along with Plaintiff Patricia Burk, had a residential home loan that was secured by a mortgage originated/serviced by Defendants for real property located in Columbus, Ohio.

13. Plaintiff Patricia Burk is a citizen of Ohio and she, along with Plaintiff Kristi Burk, had a residential home loan that was secured by a mortgage originated/serviced by Defendants for real property located in Columbus, Ohio.

14. Defendant KeyBank, N.A., is a National Association under the laws of the United States with a principal place of business in Cleveland, Ohio. Among other things, KeyBank originates and periodically sells commercial and residential mortgage loans but continues to service those loans for the buyers.[4]

[4] KeyCorp 2021 Annual Report, https://s23.q4cdn.com/646737342/files/doc_financials/2021/ar/KEY-Final-2021-Annual-Report-w-10K.pdf. KeyCorp is an Ohio corporation with a principal place of business in Cleveland, Ohio.

15. Defendant Overby-Seawell Co. is a Georgia corporation with a principal place of business in Kennesaw, Georgia. OSC is a vendor of KeyBank that provides KeyBank ongoing verification regarding residential mortgage clients' maintenance of property insurance.

16. The Court has original jurisdiction under the Class Action Fairness Act ("CAFA"), 28 U.S.C. § 1332(d)(2), because this is a Class action involving 100 or more Class members and the amount in controversy exceeds $5,000,000, exclusive of interest and costs. Many members of the Class, including Plaintiffs, are citizens of different states from Defendants.

17. Venue is proper in this District under 28 U.S.C. §§ 1391(a)(2), 1391(b)(2), and 1391(c)(2) as a substantial part of the events giving rise to the claims emanated from activities within this District, and Defendants conduct substantial business in this District.

## GENERAL ALLEGATIONS

### *The Data Breach*

18. In its August 26, 2022 notice to Plaintiffs and Class members ("Notice Letter"), Defendants state that an unauthorized external party gained remote access to their network and July 5, 2022, acquired information from Plaintiffs and Class members. A true and correct copy of the Notice Letter is attached as **Exhibit 1**.

19. Information pertaining to Plaintiffs' and Class members' KeyBank mortgage was part of the data acquired by an unauthorized external party in the Data Breach.

20. The specific information that was acquired includes: name, mortgage property address, mortgage account number(s) and mortgage account information, phone number, property information, the first eight digits of Social Security numbers, and home insurance policy number and home insurance information.

21. Notably, OSC is investigating this incident with the assistance of third-party cybersecurity experts. Because the investigation is not yet completed as of the filing of this Complaint, additional items of PII or facts may be uncovered or have already been uncovered and not disclosed.

22. Since discovering the Data Breach, Defendants "enhanced security monitoring tools across their network" —actions that should have been employed in the first place—and which would have prevented or limited the impact of the Data Breach.

23. More than one month after Defendants discovered the Data Breach and notified law enforcement, Defendants publicly announced the Data Breach and notified those who were placed at risk of identity theft. Defendant sent notices to various states' Attorneys General and to persons whose PII was acquired by criminals in the Data Breach.

24. Defendants advised in the Notice Letter that Class members should obtain credit monitoring and identity theft protection services to help them detect possible misuse of PII. *See* Exhibit 1.

25. As a result of the Data Breach, Plaintiffs and Class members have been and must continue to be vigilant and review their credit reports for incidents of identity theft, and educate themselves about security freezes, fraud alerts, and other steps to protect themselves against identity theft.

***Industry Standards for Data Security***

26. Defendants are aware of the importance of safeguarding Plaintiffs' and Class members' PII, that by virtue of their business they place Plaintiffs' and Class members' PII at risk of being targeted by hackers.

27. Defendants are aware that the PII that they collect, organize, and store, can be used by criminals to engage in crimes such as identity fraud and theft using Plaintiffs' and Class members' PII.

28. Because of Defendants' failure to implement, maintain, and comply with necessary cybersecurity requirements, Defendants were unable to protect Plaintiffs' and Class members' information and confidentiality, and protect against obvious and readily foreseeable threats to information security and confidentiality. As a proximate result of such failures, criminals gained unauthorized access to Defendants' network unimpeded and acquired Plaintiffs' and Class members' personal and financial information in the Data Breach without being stopped.

29. Only after the attack was completed did Defendants begin to undertake basic steps recognized in the industry to protect Plaintiffs and Class members' PII.

30. Defendants were unable to prevent the Data Breach, and were unable to detect the unauthorized access to vast quantities of sensitive and protected files containing protected information of Plaintiffs and Class members. Discovery on Defendants, law enforcement investigators, and private investigators, will reveal more specific facts about Defendants' deficient and unreasonable security procedures.

31. Security standards commonly accepted among businesses that store personal and financial information using the Internet include, without limitation:

a) Maintaining a secure firewall configuration;

b) Monitoring for suspicious or irregular traffic to servers;

c) Monitoring for suspicious credentials used to access servers;

d) Monitoring for suspicious or irregular activity by known users;

e) Monitoring for suspicious or unknown users;

f) Monitoring for suspicious or irregular server requests;

g) Monitoring for server requests for personal and financial information;

h) Monitoring for server requests from VPNs; and

i) Monitoring for server requests from Tor exit nodes.

32. The U.S. Federal Trade Commission ("FTC") publishes guides for businesses for cybersecurity[5] and protection of personal and financial information[6] which includes basic security standards applicable to all types of businesses.

33. The FTC recommends that businesses:

a) Identify all connections to the computers where you store sensitive information;

b) Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

c) Do not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;

d) Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;

e) Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

f) Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;

---

[5] *See* F.T.C., *Start with Security: A Guide for Business*, (June 2015), https://www.ftc.gov/system/files/documents/plain-language/pdf0205-startwithsecurity.pdf (*last accessed* July 23, 2020).

[6] *See* F.T.C., *Protecting Personal Information: A Guide for Business*, (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_protecting personalinformation.pdf (*last accessed* July 23, 2020).

g) Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;

h) Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day, and

i) Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

34. The FTC has brought enforcement actions against businesses for failing to adequately and reasonably protect customer information, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTC Act"), 15 U.S.C. § 45. Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.[7]

35. Because Defendants were entrusted with consumers' personal and financial information, they had and have a duty to keep the PII secure.

36. Plaintiffs and Class members reasonably expect that when they provide their personal and financial information to a company, the company will safeguard their personal and financial information.

[7] F.T.C., *Privacy and Security Enforcement: Press Releases*, https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/privacy-security-enforcement (*last accessed* July 15, 2020).

37. Despite Defendants' obligations, Defendants failed to upgrade and maintain their data security systems in a meaningful way so as to prevent the Data Breach.

38. Specifically, in breach of their duties, Defendants failed to:

a) Replace email filtering tools, malware software, and Internet monitoring tools with more robust solutions that utilize artificial intelligence ("AI") to detect and block known and newly introduced malware;

b) Block all inbound and outbound Internet, email, and network traffic to foreign countries;

c) Maintain a secure firewall configuration;

d) Monitor for suspicious or irregular traffic to servers;

e) Monitor for suspicious credentials used to access servers;

f) Monitor for suspicious or irregular activity by known users;

g) Monitor for suspicious or unknown users;

h) Monitor for suspicious or irregular server requests;

i) Monitor for server requests for personal and financial information;

j) Monitor for server requests from VPNs;

k) Monitor for server requests from Tor exit nodes;

l) Identify all connections to the computers where Defendants store sensitive information;

m) Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;

n) Scan computers on Defendants' network to identify and profile the operating system and open network services, and disable services that are not needed to prevent hacks or other potential security problems;

o) Pay particular attention to the security of Defendants' web applications—the software used to give information to visitors to its websites and to retrieve information from them;

p) Use a firewall to protect Defendants' computers from hacker attacks while it is connected to a network, especially the Internet;

q) Determine whether a border firewall should be installed where Defendants' network connects to the Internet;

r) Monitor incoming traffic for signs that someone is trying to hack in, and

s) Monitor outgoing traffic for signs of a data breach.

39. KeyBank also negligently entrusted duties to safeguard Plaintiffs' and Class members' PII to OSC without adequately monitoring, inspecting, and controlling OSC's data security practices.

40. KeyBank also negligently supervised OSC and failed to require OSC to implement, maintain, and upgrade sufficiently its data security systems and protocols.

41. Had Defendants properly maintained their systems and adequately protected them, they could have prevented the Data Breach.

***Defendants Owed Duties to Plaintiffs and Class Members to Adequately Safeguard Their PII***

42. Defendants are aware of the importance of security in maintaining personal information (particularly sensitive personal and financial information), and the value consumers place on keeping their PII secure.

43. Defendants owe duties to Plaintiffs and the Class members to maintain adequate security and to protect the confidentiality of their PII.

44. Defendants owe a further duty to their customers to immediately and accurately notify them of a breach of their systems to protect them from identity theft and other misuse of their personal data and to take adequate measures to prevent further breaches.

***The Categories of PII at Issue Here Are Particularly Valuable to Criminals***

45. Businesses that store sensitive PII are likely to be targeted by cyber criminals.

Credit card and bank account numbers are tempting targets for hackers. However, information such as Social Security numbers are even more attractive to hackers because they are not easily destroyed and can be easily used to perpetrate identity theft and other types of fraud.

46. The unauthorized disclosure of Social Security numbers can be particularly damaging, because Social Security numbers cannot easily be replaced. In order to obtain a new Social Security number a person must prove, among other things, that he or she continues to be disadvantaged by the misuse. Thus, no new Social Security number can be obtained until the damage has been done.

47. Furthermore, as the Social Security Administration ("SSA") warns:

> Keep in mind that a new number probably will not solve all your problems. This is because other governmental agencies (such as the IRS and state motor vehicle agencies) and private businesses (such as banks and credit reporting companies) likely will have records under your old number. Along with other personal information, credit reporting companies use the number to identify your credit record. So using a new number will not guarantee you a fresh start. This is especially true if your other personal information, such as your name and address, remains the same.
>
> If you receive a new Social Security Number, you should not be able to use the old number anymore.
>
> For some victims of identity theft, a new number actually creates new problems. If the old credit information is not associated with your new number, the absence of any credit history under the new number may make more difficult for you to get credit.[8]

48. Here, the unauthorized access by the hackers left the cyber criminals with the tools to perform the most thorough identity theft—they have obtained all the essential PII to mimic the identity of the user. Plaintiffs and Class members' stolen personal data represents essentially one-stop shopping for identity thieves.

[8] SSA, Identity Theft and Your Social Security Number, SSA Publication No. 05-10064 (Dec. 2013), *available at* http://www.ssa.gov/pubs/EN-05-10064.pdf (last visited 3/26/2021).

49. According to the FTC, identity theft wreaks havoc on consumers' finances, credit history, and reputation and can take time, money, and patience to resolve.[9] Identity thieves use stolen personal information for a variety of crimes, including credit card fraud, phone or utilities fraud, and bank and finance fraud.[10]

50. More recently the FTC has released its updated publication on protecting PII for businesses, which includes instructions on protecting PII, properly disposing of PII, understanding network vulnerabilities, implementing policies to correct security problems, using intrusion detection programs, monitoring data traffic, and having in place a response plan.

51. The FTC has, upon information and belief, brought enforcement actions against businesses for failing to protect PII. The FTC has done this by treating a failure to employ reasonable measures to protect against unauthorized access to PII as a violation of the FTC Act, 15 U.S.C. § 45.

52. General policy reasons support such an approach. A person whose personal information has been compromised may not see any signs of identity theft for *years*. According to a U.S. Government Accountability Office report:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.[11]

---

[9] *See Taking Charge, What to Do If Your Identity is Stolen*, FTC, 3 (2012), http://www.consumer.ftc.gov/articles/pdf-0009-taking-charge.pdf (last visited 3/26/2021).

[10] *Id.* The FTC defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority." 16 CFR § 603.2. The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, social security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number." *Id.*

[11] *See* http://www.gao.gov/new.items/d07737.pdf at 29 (last visited 11/13/2020).

53. Companies recognize that PII is a valuable asset. Indeed, PII is a valuable commodity. A "cyber black-market" exists in which criminals openly post stolen Social Security numbers and other PII on a number of Internet websites. Plaintiffs' and Class members' personal data that was stolen has a high value on both legitimate and black markets.

54. At an FTC public workshop in 2001, then-Commissioner Orson Swindle described the value of a consumer's personal information as follows:

> The use of third party information from public records, information aggregators and even competitors for marketing has become a major facilitator of our retail economy. Even [Federal Reserve] Chairman [Alan] Greenspan suggested here some time ago that it's something on the order of the life blood, the free flow of information.[12]

55. Individuals rightfully place a high value not only on their PII, but also on the privacy of that data. Researchers have already begun to shed light on how much individuals value their data privacy – and the amount is considerable.

56. Notably, one study on website privacy determined that U.S. consumers valued the restriction of improper access to their personal information – the very injury at issue here – between $11.33 and $16.58 per website. The study also determined that "[a]mong U.S. subjects, protection against errors, improper access, and secondary use of personal information is worth US$30.49 – 44.62."[13] This study was done in 2002. The sea-change in how pervasive the Internet is in everyday lives since then indicates that these values—when associated with the loss of PII to bad actors—would be exponentially higher today.

57. Identity thieves may commit various types of crimes such as immigration fraud,

---

[12] FEDERAL TRADE COMMISSION, *The Information Marketplace: Merging and Exchanging Consumer Data*, *transcript available* at http://www.ftc.gov/news-events/events-calendar/2001/03/information-marketplace-merging-exchanging-consumer-data (last visited 11/13/2020).
[13] Hann, Hui, *et al*, The Value of Online Information Privacy: Evidence from the USA and Singapore, at 17. Oct. 2002, available at https://www.comp.nus.edu.sg/~ipng/research/privacy.pdf (last visited 3/26/2021).

obtaining a driver's license or identification card in the victim's name but with another's picture, and/or using the victim's information to obtain a fraudulent tax refund or fraudulent unemployment benefits. The United States government and privacy experts acknowledge that it may take years for identity theft to come to light and be detected.

58. As noted above, the disclosure of Social Security numbers in particular poses a significant risk. Criminals can, for example, use Social Security numbers to create false bank accounts or file fraudulent tax returns.[14] Plaintiffs and Class members will and already have spent time contacting various agencies, such as the Internal Revenue Service and the Social Security Administration. They also now face a real and imminent substantial risk of identity theft and other problems associated with the disclosure of their Social Security number and will need to monitor their credit and tax filings for an indefinite duration.

59. Again, because the information Defendants allowed to be compromised and taken is of such a durable and near-permanent quality, the harms to Plaintiffs and the Class will continue to grow, and Plaintiffs and the Class will continue to be at substantial risk for further imminent and future harm.

***Damages From Data Breaches***

60. According to Javelin Strategy & Research, in 2017 alone over 16.7 million individuals were affected by identity theft, causing $16.8 billion to be stolen.

61. Consumers place a high value not only on their personal and financial information, but also on the privacy of that data. This is because identity theft causes "significant negative financial impact on victims" as well as severe distress and other strong emotions and physical

[14] When fraudulent tax returns are filed, the requirements for a legitimate taxpayer to file their tax returns with the IRS increase, including the necessity to obtain and utilize unique PIN numbers just to be able to file a tax return.

reactions.

62. The United States Government Accountability Office explains that "[t]he term 'identity theft' is broad and encompasses many types of criminal activities, including fraud on existing accounts—such as unauthorized use of a stolen credit card number—or fraudulent creation of new accounts—such as using stolen data to open a credit card account in someone else's name." *See In re Zappos.com, Inc.*, 888 F.3d 1020, 1024 (9th Cir. 2018). The GAO Report notes that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."

63. The FTC recommends that identity theft victims take several steps to protect their personal and financial information after a data breach, including contacting one of the credit bureaus to place a fraud alert (consider an extended fraud alert that lasts for 7 years if someone steals their identity), reviewing their credit reports often, contacting companies to remove fraudulent charges from their accounts, placing a credit freeze on their credit, and correcting their credit reports.

64. Identity thieves use stolen personal and financial information for "various types of criminal activities, such as when personal and financial is used to commit fraud or other crimes," including "credit card fraud, phone or utilities fraud, bank fraud and government fraud." *In re Zappos.com, Inc.*, 888 F.3d at 1024. The information exfiltrated in the Data Breach can also be used to commit identity theft by placing Plaintiffs and Class members at a higher risk of "phishing," "vishing," "smishing," and "pharming," which are which are ways for hackers to exploit information they already have to get even more personally identifying information through unsolicited email, text messages, and telephone calls purportedly from a legitimate company requesting personal, financial, and/or login credentials.

65. There may be a time lag between when harm occurs versus when it is discovered, and also between when personal and financial information is stolen and when it is used. According to the U.S. Government Accountability Office, which conducted a study regarding data breaches:

> [L]aw enforcement officials told us that in some cases, stolen data may be held for up to a year or more before being used to commit identity theft. Further, once stolen data have been sold or posted on the Web, fraudulent use of that information may continue for years. As a result, studies that attempt to measure the harm resulting from data breaches cannot necessarily rule out all future harm.
>
> *See* GAO Report, at p. 29.

66. Personal and financial information is such a valuable commodity to identity thieves that once the information has been compromised, criminals often trade the information on the "cyber blackmarket" for years.

67. Thus, there is a strong probability that entire batches of stolen information have been dumped on the black market, or are yet to be dumped on the black market, meaning Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future.

68. Data breaches are preventable. As Lucy Thompson wrote in the DATA BREACH AND ENCRYPTION HANDBOOK, "In almost all cases, the data breaches that occurred could have been prevented by proper planning and the correct design and implementation of appropriate security solutions." She added that "[o]rganizations that collect, use, store, and share sensitive personal data must accept responsibility for protecting the information and ensuring that it is not compromised . . . ."

69. "Most of the reported data breaches are a result of lax security and the failure to create or enforce appropriate security policies, rules, and procedures. . . . Appropriate information security controls, including encryption, must be implemented and enforced in a rigorous and

disciplined manner so that a data breach never occurs."

70. Indeed, here Defendants "Deployed enhanced security monitoring tools across their network after the Data Breach," but should have implemented them to prevent the Data Breach.

71. The types of information Defendants acknowledge were stolen by the criminals are sufficiently sensitive and valuable to identity thieves and criminals in perpetrating identity crimes. Defendants state that Plaintiffs and all Class members' names, mortgage property address, mortgage account number(s) and mortgage account information, phone number, property information, 8-digits of Social Security numbers, and home insurance policy number and home insurance information were accessed and acquired. *See* Exhibit 1. This information is essentially immutable and can be used to perpetrate scams, victimize the persons who own the information, and commit identity theft and fraud.

72. The types of information compromised in the Data Breach are immutable. Plaintiffs and Class members are not able to change them or simply cancel them, like a credit card, to avoid harm or fraudulent use of the information. Just like a birthdate or a mother's maiden name, these pieces of information cannot be changed by logging into a website and changing them in settings, and they can be used alone or in conjunction with other pieces of information to commit serious fraud.

73. Criminals can use the information to devise and employ phishing and social engineering schemes capitalizing on the genuine information stolen from Defendants to send fraudulent mail, emails, and other communications to Plaintiffs and Class members that look authentic, but which are designed to lure them into paying money or providing other information that the criminals can use to steal money. For example, homeowners with trouble paying their loan payments may experience scams targeting them.

74. According to Experian:[15]

> Mortgage Foreclosure Relief and Debt Management Scams
>
> In this type of mortgage fraud, scammers contact homeowners offering help if they can't make payments or may be falling behind on their mortgage (the primary contact is by phone with these). … Often they make promises of lower payments or making the payments for a homeowner in exchange for rent payments to their company. However, they don't actually make the mortgage payments and you may end up going into foreclosure anyway.
>
> Also known as foreclosure scams or foreclosure rescue schemes, this kind of fraud is unfortunately very common and can cost consumers a lot of Money.

75. The information stolen in the Data Breach, by itself, can also be used by criminals to perpetrate fraud that will leave Plaintiffs and Class members holding the bag. Experian explains that certain scams, including mortgage fraud, can be effectively perpetrated using only a name and loan number.[16]

> How Consumers Are Affected By Mortgage Fraud
>
> Identity theft is a particularly threatening form of mortgage fraud, as it tends to lead directly toward homeowner financial loss. For example, if an identity thief steals a homeowner's Social Security number, or intercepts the mortgage account number, he or she can use that information to take out a home equity line of credit (also known as a HELOC) worth tens of thousands of dollars, in the homeowner's name.

76. Experian explains how mortgage fraud impacts the homeowner. When the credit is provided to the fraudster:[17]

> The cash is sent to a fraudulent account established by the thief, and the homeowner is left holding the bill. Or, the fraudster could take out a second mortgage using the homeowner's stolen data information, and escape with the cash, once again leaving the debt to the homeowner.

---

[15] https://www.experian.com/blogs/ask-experian/heres-everything-you-need-to-know-about-the-risks-of-mortgage-fraud/ (last visited March 30, 2022).
[16] *Id.*
[17] *Id.*

> While any form of mortgage fraud is a serious offense, losing one's data to identity thieves can trigger a financial loss that's difficult to overcome, and that could take years to clear. Additional impacts include losing money, time, or missing out on the purchase of a dream home because you have to take additional time to deal with restoring your identity if you're the victim of mortgage fraud.

77. Identity Force explains what a thief or scammer can do with sensitive information, such as loan information and identifying details, including stealing your home:[18]

> Mortgaging Your Good Name
>
> Mortgage fraud through identity theft is a very real risk. A thief can steal your Social Security number and other identifying details, then pretend to be you to a bank or mortgage broker. The criminal might refinance your home for more than what's owed and then take the extra cash or obtain a home equity line of credit and drain that account.
>
> In some cases, you can experience house stealing through a fraudulent deed transfer. An identity thief could use stolen information to execute a transfer, which would put your property in his or her name. That means you'd legally no longer own that real estate. Since the criminal's name is on the deed, he or she would have the right to take out loans against the house. With no payments made on those loans or the mortgage, the property could even go into foreclosure.
>
> Thieves can get the information they need for these transactions by stealing your mail, getting personal details through fraudulent phone calls, or making copies of your driver's license to impersonate you. Unfortunately, sometimes it's friends and family who are the culprits (known as familiar fraud) since they may have access to files inside a home and often know many of the personal details required to impersonate you.

***Plaintiffs Received Defendants' Data Breach Notification Letter***

78. Plaintiff Aurora Murgu took out a mortgage loan for property in Westlake, Ohio. For all times relevant to this Complaint, KeyBank was the originator and/or servicer of the loan, and OSC performed services as KeyBank's vendor. Pursuant to an agreement between KeyBank and OSC, KeyBank transmitted Plaintiffs' and Class members' PII to OSC.

[18] https://www.identityforce.com/blog/home-loan-identity-theft. (last visited March 30, 2022)

79. Plaintiff James McNichol took out a mortgage loan for property in Hamburg, New York. For all times relevant to this Complaint, KeyBank was the originator and/or servicer of the loan, and OSC performed services as KeyBank's vendor. Pursuant to an agreement between KeyBank and OSC, KeyBank transmitted Plaintiffs' and Class members' PII to OSC.

80. Plaintiff Jessica McNichol took out a mortgage loan for property in Hamburg, New York. For all times relevant to this Complaint, KeyBank was the originator and/or servicer of the loan, and OSC performed services as KeyBank's vendor. Pursuant to an agreement between KeyBank and OSC, KeyBank transmitted Plaintiffs' and Class members' PII to OSC.

81. Plaintiff Kristi Burk took out a mortgage loan for property in Columbus, Ohio. For all times relevant to this Complaint, KeyBank was the originator and/or servicer of the loan, and OSC performed services as KeyBank's vendor. Pursuant to an agreement between KeyBank and OSC, KeyBank transmitted Plaintiffs' and Class members' PII to OSC.

82. Plaintiff Patricia Burk took out a mortgage loan for property in Columbus, Ohio. For all times relevant to this Complaint, KeyBank was the originator and/or servicer of the loan, and OSC performed services as KeyBank's vendor. Pursuant to an agreement between KeyBank and OSC, KeyBank transmitted Plaintiffs' and Class members' PII to OSC.

83. Plaintiffs and Class members provided Defendants with significant personal, income, and financial information that Defendants were able to acquire and to supplement by obtaining credit reports and banking information from third parties. Such information included, but is not limited to:

- Full name, mailing address, phone numbers, email address, and loan identification number;
- Co-borrower contact information, phone numbers, email address, and mailing address;

- Notations and comments concerning collections and loan servicing;
- Fee balance information;
- Information regarding insurance on the property and property details pertinent thereto;
- Loan history information, Social Security number, transaction dates, due dates, transaction amount, principal amount, end principal balance, interest, escrow amounts, check numbers, late charges, assistance amounts; details on loans in arrears;
- Tax information, including tax type, frequency, account number, and payee information;
- Credit information from consumer reports and files held by consumer reporting agencies; and
- Other information, but Plaintiffs do not know the full extent of the information Defendants have relating to Plaintiffs.

84. It is plausible to assume that the foregoing pieces of information relating to Plaintiffs and Class members were exposed, compromised, accessed, viewed without authorization, and stolen in the Data Breach by criminals. Defendants' Notice Letter indicates that broad categories of information, such as "mortgage account information" and "home insurance information" were acquired but does not provide any more particularity regarding what information those categories encompass. In addition, the Notice Letter explains that OSC continues to investigate the Data Breach as of August 26, 2022. The logical inference is that additional information regarding the Data Breach is yet to be uncovered, which may reveal additional misconduct or other fields of valuable information not already specified.

85. On or about August 26, 2022, Defendants sent the Notice Letter by mail notifying Plaintiffs that PII relating to Plaintiffs and other residential mortgage clients—including their names, mortgage property address, mortgage account number(s) and mortgage account information, phone number, property information, 8-digits of Social Security numbers, and home

insurance policy number and home insurance information—was taken by an "unauthorized external party". *See* Exhibit 1.

***Plaintiffs' and Class Members' Damages***

86. As a direct and proximate result of Defendants' conduct, Plaintiffs and Class members have been placed at an imminent, immediate, and continuing increased risk of harm from fraud and identity theft.

87. Plaintiffs and Class members have or will suffer actual injury as a direct result of the Data Breach including:

a) Spending time reviewing finding fraudulent charges and remedying fraudulent charges;

b) Purchasing credit monitoring and identity theft prevention;

c) Time and money addressing and remedying identity theft;

d) Spending time placing "freezes" and "alerts" with credit reporting agencies and, subsequently, temporarily lifting a security freeze on a credit report, or removing a security freeze from a credit report;

e) Spending time on the phone with or visiting financial institutions to dispute fraudulent charges;

f) Contacting their financial institutions and closing or modifying financial accounts compromised as a result of the Data Breach; and

g) Closely reviewing and monitoring bank accounts and credit reports for unauthorized activity for years to come.

88. Moreover, Plaintiffs and the Class members have an interest in ensuring that their personal and financial information is protected from further breaches by the implementation of security measures and safeguards, including making sure that the storage of data containing their personal and financial information is secure.

89. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class members have suffered anxiety, emotional distress, and loss of privacy.

90. As a direct and proximate result of Defendants' actions and inactions, Plaintiffs and Class members are at an increased and immediate risk of future harm, including from identity theft and fraud related to their financial accounts.

91. As a result of the Data Breach, Plaintiffs and Class members are at an imminent risk of identity theft and fraud. This risk will continue to exist for years to come, as Plaintiffs and Class members must spend their time being extra vigilant, due to Defendants' failures, to try to prevent being victimized for the rest of their lives.

92. Because Defendants presented such an easy target to cyber criminals, Plaintiffs and Class members have already been subjected to violations of their privacy, and have been exposed to a heightened and imminent risk of fraud and identity theft. Plaintiffs and Class members must now and in the future, spend time to more closely monitor their financial accounts to guard against identity theft and other fraud.

93. Plaintiffs and Class members may also incur out-of-pocket costs for, among other things, purchasing credit monitoring services or other protective measures to deter and detect identity theft.

## CLASS ACTION ALLEGATIONS

94. Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of a class of similarly situated individuals (the "Class") defined as follows:

> All individuals in the United States whose personally identifiable information was accessed in the Data Breach.

95. In addition, Plaintiffs bring this action pursuant to Fed. R. Civ. P. 23(b)(2) and (b)(3) on behalf of a subclass of similarly situated individuals in Ohio ("Ohio Subclass") defined as follows:

> All individuals in Ohio whose personally identifiable information was

accessed in the Data Breach.

96. Excluded from the Class and Ohio Subclass (collectively, "Classes") are Defendants; any entity in which Defendants have a controlling interest, is a parent or subsidiary, or which is controlled by Defendants; and the affiliates, legal representatives, attorneys, heirs, predecessors, successors, and assigns of Defendants. Also excluded are the judges and court personnel in this case and any members of their immediate families.

97. Plaintiffs reserve the right to modify and/or amend the Class and Ohio Subclass definition, including but not limited to creating subclasses, as necessary.

98. ***Numerosity***. The Classes are so numerous that joinder of all members is impracticable. KeyCorp reported $131 million in consumer mortgage income in its 2021 Annual Report, suggesting a large number of loans originated and/or serviced by Defendants.[19] The identities of all Class members are ascertainable through Defendants' records.

99. ***Commonality***. There are numerous questions of law and fact common to Plaintiffs and the Class, including the following:

- Whether and to what extent Defendants had a duty to protect the PII of Plaintiffs and Class members;
- Whether Defendants had a duty not to disclose the PII of Plaintiffs and Class members to unauthorized third parties;
- Whether Defendants had a duty not to use the PII of Plaintiffs and Class members for non-business purposes;
- Whether Defendants failed to adequately safeguard the PII Plaintiffs and Class members;
- Whether and when Defendants actually learned of the Data Breach;
- Whether Defendants adequately, promptly, and accurately informed

[19] KeyCorp Annual Report for 2021, p. 103, https://s23.q4cdn.com/646737342/files/doc_financials/2021/ar/KEY-Final-2021-Annual-Report-w-10K.pdf

Plaintiffs and Class members that their PII had been compromised;

- Whether Defendants violated the law by failing to promptly notify Plaintiffs and Class members that their PII had been compromised;
- Whether Defendants failed to implement and maintain reasonable security procedures and practices appropriate to the nature and scope of the information compromised in the Data Breach;
- Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breach to occur;
- Whether Defendants engaged in unfair, unlawful, or deceptive practices by failing to safeguard the PII of Plaintiffs and Class members;
- Whether Plaintiffs and Class members are entitled to actual damages, nominal damages, and/or exemplary damages as a result of Defendants' wrongful conduct;
- Whether Plaintiffs and Class members are entitled to restitution as a result of Defendants' wrongful conduct; and
- Whether Plaintiffs and Class members are entitled to injunctive relief to redress the imminent and currently ongoing harm faced as a result of the Data Breach.

100. ***Typicality***. Plaintiffs' claims are typical of the claims of the Class in that Plaintiffs, like all Class members, had their personal data compromised, breached and stolen in the Data Breach. Plaintiffs and Class members were injured through Defendants' uniform misconduct described in this Complaint and assert the same claims for relief.

101. ***Adequacy***. Plaintiffs and counsel will fairly and adequately protect the interests of the Class. Plaintiffs have retained counsel who are experienced in class actions and complex litigation, including data privacy litigation of this kind. Plaintiffs have no interests that are antagonistic to, or in conflict with, the interests of other members of the Class.

102. ***Predominance***. The questions of law and fact common to Class members predominate over any questions which may affect only individual members.

103. ***Superiority***. A class action is superior to other available methods for the fair and

efficient adjudication of the controversy. Class treatment of common questions of law and fact is superior to multiple individual actions or piecemeal litigation. Moreover, absent a class action, most Class members would find the cost of litigating their claims prohibitively high and would therefore have no effective remedy, so that in the absence of class treatment, Defendants' violations of law inflicting substantial damages in the aggregate would go unremedied without certification of the Class. Plaintiffs and Class members have been harmed by Defendants' wrongful conduct and/or action. Litigating this action as a class action will reduce the possibility of repetitious litigation relating to Defendants' conduct and/or inaction. Plaintiffs know of no difficulties that would be encountered in this litigation that would preclude its maintenance as a class action.

104. Class certification, therefore, is appropriate under Fed. R. Civ. P. 23(b)(3), because the above common questions of law or fact predominate over any questions affecting individual members of the Class, and a class action is superior to other available methods for the fair and efficient adjudication of this controversy.

105. Class certification is appropriate under Fed. R. Civ. P. 23(b)(2), because Defendants have acted or refused to act on grounds that apply generally to the class so that final injunctive relief or corresponding declaratory relief is appropriate respecting the class as a whole.

## FIRST CAUSE OF ACTION
**Negligence**
***(On behalf of Plaintiffs and the Class and Ohio Subclass)***
***(Against All Defendants)***

106. Plaintiffs repeat and reallege the allegations of paragraphs 1-105 with the same force and effect as though fully set forth herein.

107. Defendants' actions and inactions were of the type that would result in foreseeable, unreasonable risk of harm to Plaintiffs and Class members. Defendants knew, or should have

known, of the risks inherent in collecting and storing the personal and financial information of Plaintiffs and Class members and the importance of adequate security in storing the information. Additionally, Defendants are aware of numerous, well-publicized data breaches that exposed the personal and financial information of individuals.

108. Defendants had a common law duty to prevent foreseeable harm to Plaintiffs' and Class members' PII. This duty existed because Plaintiffs and Class members were the foreseeable and probable victims of the failure of Defendants to adopt, implement, and maintain reasonable security measures so that Plaintiffs' and Class members' personal and financial information would not be unsecured and accessible by unauthorized persons.

109. Defendants had a special relationship with Plaintiffs and Class members. Defendants were entrusted with Plaintiffs' and Class members' personal and financial information, and Defendants were in a position to protect the personal and financial information from unauthorized access.

110. The duties of Defendants also arose under section 5 of the FTC Act, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect individuals' personal and financial information by companies. Various FTC publications and data security breach orders further form the basis of the duties of Defendants.

111. Defendants had a duty to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Plaintiffs' and Class members' personal and financial information in their possession so that the personal and financial information would not come within the possession, access, or control of unauthorized persons.

112. More specifically, the duties of Defendants included, among other things, the following duties, and Defendants carelessly and negligently acted or failed to act in one or more of the following ways:

- Failing to conduct proper and reasonable due diligence over OSC and OSC's data security systems, practices, and procedures;
- Failing to conduct proper and reasonable due diligence over vendors or contractors that were the vectors of or facilitated the infiltration into the systems sorting the PII;
- Failing to maintain reasonable and appropriate oversight and audits on OSC and other vendors or contractors that were the vectors of the Data Breach;
- Failing to adopt, implement, and maintain adequate security measures for protecting an individual's personal and financial information to ensure that the information is not accessible online by unauthorized persons;
- Failing to adopt, implement, and maintain adequate security measure for deleting or destroying personal and financial information when Defendants' business needs no longer required such information to be stored and maintained; and
- Failing to adopt, implement, and maintain processes to quickly detect a data breach and to promptly act on warnings about data breaches, and notify affected persons without unreasonable delay.

113. Defendants breached the foregoing duties to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting individual's personal and financial information in their possession so that the information would not come within the possession, access, or control of unauthorized persons.

114. Defendants acted with reckless disregard for the security of the personal and financial information of Plaintiffs and the Class because Defendants knew or should have known that their data security was not adequate to safeguard the personal and financial information that was collected and stored.

115. Defendants acted with reckless disregard for the rights of Plaintiffs and the Class members by failing to promptly detect the Data Breach, and further, by failing to notify Plaintiffs and the Class members of the Data Breach in the most expedient time possible and without unreasonable delay pursuant to common law duties to provide reasonably timely and truthful data-breach notification, so that Plaintiffs and Class members could promptly take measures to protect themselves from the consequences of the unauthorized access to the personal and financial information compromised in the Data Breach.

116. As a result of the conduct of Defendants, Plaintiffs and Class members have suffered and will continue to suffer foreseeable harm. Plaintiffs and Class members have suffered actual damages including, but not limited to, imminent risk of identity theft; expenses and/or time spent on credit monitoring for a period of years; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and subsequently temporarily lifting credit freezes; and increased risk of future harm. Further, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

## SECOND CAUSE OF ACTION
**Negligence Per Se**
***(On Behalf of Plaintiffs and the Class and Ohio Subclass)***
***(Against All Defendants)***

117. Plaintiffs repeat and reallege the allegations of paragraphs 1-105 with the same force and effect as though fully set forth herein.

118. "Section 5 of the FTC Act [15 U.S.C. § 45] is a statute that creates enforceable duties, and this duty is ascertainable as it relates to data breach cases based on the text of the statute and a body of precedent interpreting the statute and applying it to the data beach context." *In re*

*Capital One Consumer Data Sec. Breach Litig.*, 488 F. Supp. 3d 374, 407 (E.D. Va. 2020). "For example, in *F.T.C. v. Wyndham Worldwide Corp.*, 799 F.3d 236, 240 (3d Cir. 2015), the United States Court of Appeals for the Third Circuit affirmed the FTC's enforcement of Section 5 of the FTC Act in data breach cases." *Capital One Data Security Breach Litigation*, 488 F. Supp. 3d at 407.

119. In addition, Plaintiffs and Class members may maintain a negligence per se claim based on conduct declared unlawful under the Safeguards Rule, 16 C.F.R. part 314, promulgated by the FTC pursuant to authority delegated by Congress under the Gramm-Leach-Bliley Act ("GLBA"), 15 U.S.C. § 6801(b), to establish standards for financial institutions relating to administrative, technical, and physical safeguards for nonpublic information, including Plaintiffs' and Class members' PII.

120. The Safeguards Rule at 16 C.F.R. § 314.4 provides:

> In order to develop, implement, and maintain your information security program, [a financial institution] shall:
>
> (a) Designate an employee or employees to coordinate your information security program.
>
> (b) Identify reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information, and assess the sufficiency of any safeguards in place to control these risks. At a minimum, such a risk assessment should include consideration of risks in each relevant area of your operations, including:

(1) Employee training and management;

(2) Information systems, including network and software design, as well as information processing, storage, transmission and disposal; and

(3) Detecting, preventing and responding to attacks, intrusions, or other systems failures.

(c) Design and implement information safeguards to control the risks you identify through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures.

(d) Oversee service providers, by:

(1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and

(2) Requiring your service providers by contract to implement and maintain such safeguards.

(e) Evaluate and adjust your information security program in light of the results of the testing and monitoring required by paragraph (c) of this section; any material changes to your operations or business arrangements; or any other circumstances that you know or have reason to know may have a material impact on your information security program.

16 C.F.R. § 314.4.

121. The Safeguards Rule is a process-based rule drafted using intentionally broad language and not incorporating any specific information security standard or framework to allow financial institutions flexibility to "shape the information security programs to their particular business and to allow the programs to adapt to changes in technology and threats to the security and integrity of customer information."[20]

122. Defendants are financial institutions within the meaning of the GLBA.

123. Plaintiffs' and Class members' PII was and is nonpublic personal information and customer information.

124. Defendants committed unlawful acts by failing to comply with the requirements of the Safeguards Rule, including but not limited to, failing to:

- Upgrade and maintain data security systems in a meaningful way so as to prevent the Data Breach;
- Replace email filtering tools, malware software, and Internet monitoring tools with more robust solutions that utilize artificial intelligence ("AI") to detect and block known and newly introduced malware;
- Block all inbound and outbound Internet, email, and network traffic to foreign countries;
- Maintain a secure firewall configuration;
- Monitor for suspicious or irregular traffic to servers;
- Monitor for suspicious credentials used to access servers;
- Monitor for suspicious or irregular activity by known users;
- Monitor for suspicious or unknown users;
- Monitor for suspicious or irregular server requests;

[20] Fed. Trade Comm'n, Standards for Safeguarding Customer Information, 84 Fed. Reg. 13158, 13159 (Apr. 4, 2019), also available at https://www.federalregister.gov/documents/2019/04/04/2019-04981/standards-for-safeguarding-customer- information (last visited Nov. 16, 2021).

- Monitor for server requests for personal and financial information;
- Monitor for server requests from VPNs;
- Monitor for server requests from Tor exit nodes;
- Identify all connections to the computers where Defendants store sensitive information;
- Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;
- Scan computers on Defendants' network to identify and profile the operating system and open network services, and disable services that are not needed to prevent hacks or other potential security problems;
- Pay particular attention to the security of Defendants' web applications—the software used to give information to visitors to their websites and to retrieve information from them;
- Use a firewall to protect Defendants' computers from hacker attacks while it is connected to a network, especially the Internet;
- Determine whether a border firewall should be installed where Defendants' network connects to the Internet;
- Monitor incoming traffic for signs that someone is trying to hack in;
- Monitor outgoing traffic for signs of a data breach;
- Identify all connections to the computers where they store sensitive information;
- Assess the vulnerability of each connection to commonly known or reasonably foreseeable attacks;
- Not store sensitive consumer data on any computer with an internet connection unless it is essential for conducting their business;
- Scan computers on their network to identify and profile the operating system and open network services. If services are not needed, they should be disabled to prevent hacks or other potential security problems. For example, if email service or an internet connection is not necessary on a certain computer, a business should consider closing the ports to those services on that computer to prevent unauthorized access to that machine;
- Pay particular attention to the security of their web applications—the software used to give information to visitors to their websites and to retrieve

information from them. Web applications may be particularly vulnerable to a variety of hack attacks;

- Use a firewall to protect their computers from hacker attacks while it is connected to a network, especially the internet;
- Determine whether a border firewall should be installed where the business's network connects to the internet. A border firewall separates the network from the internet and may prevent an attacker from gaining access to a computer on the network where sensitive information is stored. Set access controls—settings that determine which devices and traffic get through the firewall—to allow only trusted devices with a legitimate business need to access the network. Since the protection a firewall provides is only as effective as its access controls, they should be reviewed periodically;
- Monitor incoming traffic for signs that someone is trying to hack in. Keep an eye out for activity from new users, multiple log-in attempts from unknown users or computers, and higher-than-average traffic at unusual times of the day; and
- Monitor outgoing traffic for signs of a data breach. Watch for unexpectedly large amounts of data being transmitted from their system to an unknown user. If large amounts of information are being transmitted from a business' network, the transmission should be investigated to make sure it is authorized.

125. Plaintiffs and Class members are in the group of persons the FTC Act and Safeguards Rule were enacted and implemented to protect, and the harms they suffered in the Data Breach as a result of Defendants' violations of the FTC Act and Safeguards Rules were the types of harm they were designed to prevent.

126. As a result of the conduct of Defendants that violated the FTC Act and the Safeguards Rule, Plaintiffs and Class members have suffered and will continue to suffer foreseeable harm. Plaintiffs and Class members have suffered actual damages including, but not limited to, imminent risk of identity theft; expenses and/or time spent on credit monitoring for a period of years; time spent scrutinizing bank statements, credit card statements, and credit reports; time spent initiating fraud alerts and credit freezes and subsequently temporarily lifting credit

freezes; and increased risk of future harm. Further, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm including, but not limited to, anxiety, emotional distress, loss of privacy, and other economic and non-economic losses.

## PRAYER FOR RELIEF

WHEREFORE Plaintiffs, individually and on behalf of the Classes, requests that the Court:

A. Certify this case as a class action on behalf of the Classes defined above, appoint Plaintiffs as the Class representatives, and appoint the undersigned counsel as Class counsel;

B. Award declaratory, injunctive and other equitable relief as is necessary to protect the interests of Plaintiffs and Class members;

C. Award restitution and damages to Plaintiffs and Class members in an amount to be determined at trial;

D. Award Plaintiffs and Class members their reasonable litigation expenses and attorneys' fees to the extent allowed by law;

E. Award Plaintiffs and Class members pre- and post-judgment interest, to the extent allowable; and

F. Award such other and further relief as equity and justice may require.

## DEMAND FOR JURY TRIAL

Plaintiffs demand a trial by jury of any and all issues in this action so triable of right.

Plaintiffs DANIEL BOZIN, as Executor of the Estate of Aurora Murgu, and individually, JAMES MCNICHOL, JESSICA MCNICHOL, KRISTI BURK, and PATRICIA BURK, individually and on behalf of all others similarly situated,

By: */s/ Marc E. Dann*
Marc E. Dann (0039425)
Brian D. Flick (0081605)
**DannLaw**

15000 Madison Avenue
Lakewood, OH 44107
Telephone: (216) 373-0539
Facsimile: (216) 373-0536
*notices@dannlaw.com*

Thomas A. Zimmerman, Jr.
(admitted *pro hac vice*)
Jeffrey D. Blake
(admitted *pro hac vice*)
**Zimmerman Law Offices, P.C.**
77 W. Washington Street, Suite 1220
Chicago, Illinois 60602
(312) 440-0020 telephone
(312) 440-4180 facsimile
*www.attorneyzim.com*
*firm@attorneyzim.com*

*Counsel for Plaintiffs and the Class and Subclass*